Exhibit 15

WSP Manual

Alpine Securities Corporation

April 11, 2013

TABLE OF CONTENTS

1. any indictment, information or other criminal complaint or plea agreement for conduct reportable under paragraph (a)(1)(E) of this Rule;
2. any complaint in which a member is named as a defendant or respondent in any securities- or commodities-related private civil litigation, or is named as a defendant or respondent in any financial-related insurance private civil litigation;
3. any securities- or commodities-related arbitration claim, or financial-related insurance arbitration claim, filed against a member in any forum other than the FINRA Dispute Resolution forum;
4. any indictment, information or other criminal complaint, any plea agreement, or any private civil complaint or arbitration claim against a person associated with a member that is reportable under question 14 on Form U4, irrespective of any dollar thresholds Form U4 imposes for notification, unless, in the case of an arbitration claim, the claim has been filed in the FINRA Dispute Resolution forum.

3.14 Money Laundering

[FINRA Rule 3310; Bank Secrecy Act]

This section provides a brief overview of the employee's responsibilities concerning the prevention and detection of money laundering. Please refer to the chapter titled "*Anti-Money Laundering (AML) Program*" for more detailed information about Alpine's AML Program.

3.14.1 Reports Of AML Non-Compliance And Other Potential Crimes

All employees are obligated to promptly report to the AML Compliance Officer or designee any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of Alpine. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with Alpine, a customer, or prospective customer) are required to be reported. This includes suspicion that Alpine is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the Bank Secrecy Act reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to be attentive and alert to the red flags and report to the AML Compliance Officer or designee any new or existing customers who may be engaged in violations of anti-money laundering regulations.

SAR reports: By law, Alpine and its employees cannot disclose to the customer or anyone other than authorized parties that it has filed a SAR or provide information that would reveal the existence of a SAR. Questions regarding SAR filings should be referred to Compliance. If you become aware of an unauthorized disclosure of an SAR or you receive a subpoena for an SAR, **immediately contact the Compliance Department**. Designated Compliance personnel will be responsible for contacting FINCEN to report the unauthorized disclosure.

3.14.2 Identity Theft

Identity thieves use someone's personal identifying information to open new accounts and misuse existing accounts. Alpine has established an Identity Theft Prevention Program (ITPP) to help detect and prevent identity theft. Many elements of detecting or preventing identity theft utilize similar techniques to that of the anti-money laundering (AML) requirements included within these policies.

The ITPP is based on identifying "red flags" which may indicate an occurrence of identity theft. ***It is the responsibility of all employees to be attentive and alert to the red flags and report to the AML Compliance Officer any new or existing customers who may be engaged in violations of***

anti-money laundering regulations, identity theft or who have reported an instance of identity theft.

For a list of potential identity theft red flags, refer to the section titled "*Red Flag Identification and Detection Grid*" located in the ***Identity Theft Prevention Program (FTC Fact Act Red Flags Rule)*** section.

3.15 Emergency Business Recovery Procedures

[FINRA Rule 4370]

Alpine has a *Business Continuity Plan* ("BCP") that assigns responsibilities and outlines procedures in the event of a disaster, emergency or pandemic which impacts the ability of Alpine to continue conducting business (also termed a "significant business disruption"). Examples of a significant business disruption include a regional power outage; disruption at another company that provides services critical to Alpine; and destruction of an office or other facilities by natural causes or by other means. The BCP designates employees who are responsible for employee safety and protection of firm property, records, and customer assets.

In the event of a disruption, employees will be given instructions by authorized personnel. Depending on the nature of the emergency, it may be necessary to use alternate communication systems; transfer personnel and/or business activities to alternate office space; or transfer Alpine's business to other brokerage firms or financial institutions until normal operations can be resumed.

Alpine has established procedures for contacting employees in the event of an emergency. If Alpine conducts a test of its emergency procedures, all employees are required to participate as if the emergency were real. Past emergencies affecting the securities industry have shown that preparedness and cooperation are key to maximizing the safety of employees and minimizing business interruptions. It is important for all employees to follow instructions from senior management and other authorized key personnel during any drill or when an emergency occurs.

Questions regarding Alpine's Business Continuity Plan may be referred to the Chief Operating Officer.

Responsibility	• COO
Resources	• Business Continuity Records
Frequency	• Annually or as required
Action	• Administer the Business Continuity Plan • Perform annual tests for compliance with the policy
Record	• Copies of Alpine's business continuity plan • Copies of dates in which the plan is tested

[Insert Section Here]

9 ANTI-MONEY LAUNDERING (AML) PROGRAM

[FINRA Rule 3310; Bank Secrecy Act]

Money laundering is a serious crime potentially related to the funding of terrorist activities. It is the subject of extensive federal regulations that impose requirements on financial institutions, such as broker-dealers and their employees, to detect and prevent potential money laundering activities. Actions to detect and prevent money laundering is an obligation of each employee of Alpine.

Money laundering is the movement of criminally derived funds to conceal the true source, ownership, or use of the funds. The funds are filtered through a maze or series of transactions, so the funds are "cleaned" to look like proceeds from legal activities.

In general, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash profits derived from criminal activity are converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to separate further the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund further criminal or legitimate activities.

Engaging in money laundering is a federal crime with severe penalties for those engaged in the associated criminal activities and those who facilitate, intentionally or inadvertently, money laundering. It is important that Alpine, as well as all employees, remain diligent and active participants in Alpine's anti-money laundering (AML) program.

This chapter explains Alpine's Anti-Money Laundering (AML) Program. An explanation of money laundering and guidance for all employees to detect money laundering is included in this chapter. These policies will be updated and appropriate procedures and action effected when new rules are adopted.

9.1 Background

The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA), and its accompanying regulation, is a tool the U.S. government uses to fight drug trafficking, money

laundering, and other crimes. Congress enacted the BSA to prevent financial service providers (such as banks and broker-dealers) from being used as intermediaries for, or to hide the transfer or deposit of, money derived from criminal activity. Money laundering schemes may include the use of wire transfers, cash, bearer instruments, travelers' checks, money orders, cashiers' checks, and other negotiable instruments.

Alpine is required to comply with the reporting, recordkeeping, and record retention requirements of the BSA. The requirements govern the payment, receipt, or transfer of currency within, into and out of the U.S. and foreign financial transactions and accounts.

9.2 Shell Companies

[FINCen advisory on shell companies: http://www.fincen.gov/AdvisoryOnShells_FINAL.pdf]

Shell companies may represent potential money laundering risks. "Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. It is important for employees to be aware of the risks involved in dealing with shell companies.

Most shell companies are formed for legitimate business purposes such as to hold stock or intangible assets of another business entity or to facilitate domestic and cross-border currency and asset transfers and corporate mergers. Unfortunately, shell companies have become common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate, and ownership and transactional information can be concealed from regulatory and law enforcement authorities. Most states do not collect or require disclosure of ownership information at the formation stage or after.

Agents, also known as intermediaries or nominee incorporation services (NIS), can play a central role in the formation and maintenance of shell companies. Agents and NIS firms offer a wide range of services that may include offering an office address, mail-forwarding services, local telephone listings, and other services that may give the appearance of a locally-established business. Some agents and NIS firms also provide nominee services which can preserve a client's anonymity. Some risk indicators of shell companies potentially engaged in money laundering are:

- An inability to obtain (through Internet searches, commercial database searches, or direct inquiries to the company's foreign correspondent bank) information necessary to identify originators or beneficiaries of wire transfers.
- A foreign correspondent bank exceeds the anticipated volume projected in its client profile for wire transfers in a given period or an individual company exhibits a high amount of sporadic activity that is inconsistent with normal business patterns.
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or service number.
- Goods or services of the company do not match the company's profile based on information previously provided.
- Transacting businesses share the same address, provide only a registered agent's address, or raise other address-related inconsistencies.
- An unusually large number and variety of beneficiaries receive wire transfers from one company.
- Frequent involvement of beneficiaries located in high-risk, offshore financial centers.
- Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.

9.3 Penalties

Participation in a money laundering scheme or the knowing receipt of proceeds from criminal activities is a crime. Alpine and its employees are subject to severe criminal, civil, and regulatory penalties if they facilitate or participate in money laundering activities. Violations by employees may result in internal disciplinary action including termination.

An employee may be deemed to be facilitating or participating in money laundering by engaging in a transaction with a customer (accept a deposit, arrange a withdrawal, effect a trade, *etc.*) when he or she is aware of, or willfully ignores, the fact that the customer is engaged in illegal activities.

9.4 AML Compliance Officer

[NASD Rule 1160; FINRA Rule 3310(d) and 3310.02]

Responsibility	• AML Compliance Officer
Resources	• Computer reports and other programs developed for the Program • Internal audits or outside audits of the Program • Regulations and rules for broker-dealer anti-money laundering programs • OFAC web site • Other sites and resources available
Frequency	• Annual - review policies and procedures • Annual and more frequently, as needed - develop and schedule AML education for employees • As needed - update program and provide revisions to senior management for review and approval of material changes. Non-material changes to the AML Policy will not require senior management approval. • Annually - review AML contact information on file with FINRA • Ongoing - review new regulations • Ongoing - monitor activity
Action	• Develop and update Alpine's anti-money laundering program • Obtain senior management approval for any material changes to the program and any material changes to the policy • Monitor (or designate monitoring) the activity of Alpine, its associated persons, and customers to reasonably detect and prevent money laundering activities • Develop AML education program for employees and schedule training • File required reports • Retain required records • Provide contact information to FINRA and update contact information if necessary
Record	• Designation of AML Compliance Officer • Current and past copies of anti-money laundering program with senior management approval, when and where senior management approval is required • Records of AML education including who attended, date of training, and material covered

	• Reports filed • Other records to be retained, as listed in the Program

Alpine has designated an AML Compliance Officer who is responsible for overseeing Alpine's anti-money laundering program, developing policies, procedures, and internal controls reasonably designed to achieve compliance with AML rules and regulations. Contact the AML Compliance Officer whenever you have questions about Alpine's program, a current or prospective account, or activities or transactions that raise questions about potential money laundering activities. You may also provide information anonymously to the AML Compliance Officer. The AML Compliance Officer is responsible for investigating suspected money laundering activities and taking corrective action when necessary.

9.5 Independent Testing

[FINRA Rule 3310.01]

Responsibility	• AML Compliance Officer
Resources	• Policies and procedures • Independent testing results
Frequency	• Annual - schedule, conduct, and follow up testing (unless firm qualifies for testing every two years)
Action	• Identify person(s) to conduct testing • Conduct testing • Report results to CEO in annual compliance report • Revise policies and procedures as necessary • Conduct follow-up to determine corrective action has been taken
Record	• Independent testing results including who conducted and dates of review • Report to CEO • Record of changes to policies and procedures resulting from testing • Record of follow-up actions

The AML Compliance Officer will be responsible for an annual (on a calendar-year basis) independent testing of Alpine's policies and procedures regarding money laundering and the effectiveness of the program, as described in this Chapter 9. The tests performed will be either by an employee of Alpine, if such employee qualifies pursuant to the SRO rules for independence set forth below, or by a qualified non-employee, third party. At the discretion of Alpine's Board of Directors, the AML Compliance Officer may be directed to conduct interim testing of Alpine's policies and procedures regarding money laundering and the effectiveness of the program, if they believe such interim tests are warranted.
SRO rules require that the person(s) conducting the independent testing of Alpine's AML program:

- is not the AML Compliance Officer
- is not performing any AML procedures that are being tested and reviewed

- is not an individual who is supervised by or otherwise reports to the AML Compliance Officer or to someone who performs any AML procedures
- is knowledgeable regarding the Bank Secrecy Act, money laundering activities and related regulations

9.6 Training Program

All employees are provided with Alpine's Money Laundering policy when they are hired. In addition, ongoing education will include the firm element continuing education program, periodic circulation of Alpine's policy, and other educational programs directed at specific employees. Training will be delivered at least annually by video, intranet systems, in-person lectures, and other methods including third parties who deliver AML training.

Training will include the following, as well as other subjects identified by the AML Compliance Officer:

- How to identify red flags and signs of money laundering
- What to do once the risk is identified (how, when and to whom to escalate unusual customer activity or other red flags)
- Employees' roles in Alpine's compliance efforts and how to perform them
- Alpine's record retention policy
- Disciplinary consequences (including civil and criminal penalties) for non-compliance

The AML Compliance Officer or designee is responsible for retaining records of employees trained, the dates of training, and the subjects included in training.

9.7 OFAC List And Blocked Property

[Dept. of Treasury, various statutes; OFAC web site (http://www.treas.gov/offices/enforcement/ofac/); Foreign Assets Control Regulations For The Securities Industry (http://www.treas.gov/offices/enforcement/ofac/regulations/t11facsc.pdf)]

Responsibility	• RR for a new account • Supervisor approving new accounts • AML Compliance Officer as set forth in Chapter 1.1
Resources	• Name / Entity search based on above referenced OFAC web site • Comparison search program provided by CSS Hosted Solutions, LLC • Other sight identified below and at(*www.treas.gov/ofac*) (*www.fincen.gov*)
Frequency	• At the time that a new account is opened • Daily
Action	• RR shall perform an OFAC search for each new customer and attach results to new account card • Supervisor approving the new account shall only approve an account if an OFAC search is attached to the new

	account card. If a positive identification is made, the AML Compliance Officer shall be notified immediately • If a positive identification is found, the AML Compliance Officer shall: • 1- Block accounts subject to sanctions • 2- Cancel open orders for blocked accounts • 3- Notify the Branch Office Supervisor, the Compliance Officer, and the account's RR, when an account or security is blocked • 4- Notify OFAC by FAX within 10 days of blocking an account • 5- Notify Dreyfus Service Corporation with respect to funds in a blocked account having been swept into the Dreyfus Money Market account. • Daily, CSS Hosted Solutions, LLC will provide Alpine's AML compliance officer with an OFAC screening report. • The daily OFAC screenings report shall be initialed and dated by the AML compliance officer as evidence of its review and such report shall be retained by the AML compliance officer.
Record	• RR for each new account shall attach the OFAC search results to each customers new account card • The results of each CSS Hosted Solutions, LLC system search, subsequent OFAC searches undertaken, and any actions taken, shall be retained

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) is responsible for publishing sanctions against persons, corporations, and other entities including foreign governments that have been identified by the U.S. Government as engaging in criminal activities including drug trafficking and terrorist activities. Alpine is obligated to check its accounts against the lists of blockings to ensure it does not engage in prohibited transactions which include securities transactions and transfer of assets out of a blocked account or to a blocked person or entity. Alpine has procedures to monitor the OFAC lists and comply with requirements to block property and notify OFAC when required. Questions regarding Alpine's program should be referred to the AML Compliance Officer. More information is also available at the OFAC web site at *www.treas.gov/ofac.*

The property of sanctioned persons or entities will be blocked and transfer of assets prevented for persons or entities included on the OFAC list of blocked persons or entities. In addition, Alpine will block securities issued by sanctioned countries and other sanctioned issuers. Information about sanctions is divided into several categories including:

- Persons and entities subject to sanctions, *Special Designated Nationals and Blocked Persons* (SDN list)

- Persons and entities engaged in drug trafficking, *Specially Designated Narcotics Traffickers* (SDNTKs)
- Terrorists and terrorist organizations, *Specially Designated Terrorists* (SDTs)
- Countries, governments, and other entities subject to sanctions

OFAC requirements apply to all persons and entities under U.S. jurisdiction, including foreign branches of U.S. institutions. This also includes foreign institutions that operate in the U.S.

The term "OFAC list" in this section includes all sanctions published by OFAC even though the information may appear in multiple lists. Alpine will not permit prohibited transactions with sanctioned parties and will file reports with OFAC when necessary.

9.7.1 Prohibited Transactions

Alpine is prohibited from conducting transactions in any account on behalf of a sanctioned party or in certain blocked securities. Securities and funds may not be released and securities transactions may not be executed. Securities and funds may be deposited to a blocked account, but no securities or funds will be released until the account is no longer subject to sanctions. Funds or securities may not be transferred to sanctioned parties.

Because transactions are prohibited, all open orders for a blocked account will be cancelled.

9.7.2 Blocking Requirements

Blocking requirements are generally triggered under the following circumstances:

- An account is opened for someone included on an OFAC list.
- The owner of an existing account is added to an OFAC list.
- A security is identified in a customer account where the issuer is the subject of sanctions.
- A request is made by a customer to pay or transfer funds or securities to a blocked person or entity.

While title to blocked property remains with the blocked person or entity, transactions affecting the property (including transfer of the assets) cannot be made without authorization from OFAC. Debits to blocked accounts are prohibited, but credits may be accepted. Cash balances in blocked accounts must earn interest at commercially reasonable rates. Blocked securities may not be paid, withdrawn, transferred (even in book transfer), endorsed, guaranteed, or otherwise dealt in.

It is not a violation to open an account for a blocked person. The violation occurs when the account is not frozen and assets are allowed to transfer out of the account. In addition, OFAC restrictions may vary depending on the blocked person or entity; details of blocking requirements are explained on the OFAC web site.

9.7.3 Monitoring Procedures

Monitoring is to be conducted as follows:

- Operations personnel and Supervisors approving new accounts are provided with a list of the countries included on the OFAC countries list, to watch for new accounts to be opened for or requests to transfer funds or securities to residents of those countries. The AML Compliance Officer shall provide an updated list each month by email to all operations personnel and supervisors.
- Alpine undertakes an OFAC search utilizing the www.treas.gov/ofac web site for each new account and retains the OFAC search results in the new account file.

- Alpine continually reviews its existing accounts through the use of the OFAC screenings report provided by CSS Hosted Solutions, LLC. Additionally, on a weekly basis, Alpine undertakes an account rescreening through the use of CSS Hosted Solutions, LLC and generates an OFAC possible matches (rescreening) report. To evidence review, a report is produced that is reviewed, initialed and retained by the AML Compliance Officer.

9.7.4 Other Requests To Monitor Accounts

Regulators or law enforcement agencies may ask the industry's cooperation in identifying accounts for individuals or entities under investigation or suspected of criminal activities.

The AML Compliance Officer is responsible for responding to such requests; providing the necessary information; and retaining records of requests, reviews conducted pursuant to requests, and information provided to authorities.

9.7.5 Blocking Property And Disbursements

Any blocked account will not be permitted to engage in transactions other than the acceptance of deposits of funds or securities. Open orders of blocked accounts will be cancelled.

Disbursements of funds or securities may not be made to sanctioned parties. The AML Compliance Officer will instruct Alpine's back office to withhold requests for disbursements from blocked accounts and will maintain a log of all accounts that have been blocked.

9.7.6 Reporting Blocked Property And Legal Actions

When an account or disbursement is blocked or a blocked security is identified, OFAC will be notified within 10 days of blocking. If Alpine blocks an account or security, the AML Compliance Officer will file the necessary report with OFAC. The AML Compliance Officer will be responsible to retain copies of reports filed by Alpine in a file of blocked accounts or securities. Information to be reported includes:

- Owner or account party
- Property and property location
- Account number
- Actual or estimated value
- Date property was blocked
- Copy of the payment or transfer instructions
- Confirmation that funds have been deposited in a blocked account that is identified as blocked
- Name and phone number of Alpine's AML Compliance Officer

For rejected disbursements, the following information is to be filed:

- Name and address of the transferee financial institution
- Date and amount of the transfer
- Copy of the payment or transfer instructions
- Basis for rejection
- Name and phone number of Alpine's Compliance Officer

9.7.6.1 Annual Report Of Blocked Property

On an annual basis by September 30th, the AML Compliance Officer shall file Form TDF 90-22.50 with OFAC for any blocked property held as of June 30.

9.7.6.2 Legal Actions Involving Blocked Property

U.S. persons involved in litigation, arbitration, or other binding alternative dispute resolution proceedings regarding blocked property must provide notice to OFAC. Copies of all documents associated with the proceedings will be submitted by the AML Compliance Officer to the OFAC Chief Counsel at the U.S. Treasury Department within 10 days of their filing. In addition, information about the scheduling of any hearing or status conference will be faxed to the Chief Counsel.

9.7.7 Reporting Obligations for All Alpine Employees

All employees are obligated to promptly report to the AML Compliance Officer any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of Alpine. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with Alpine, a customer, or prospective customer) are required to be reported. This includes suspicion that Alpine is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the Bank Secrecy Act reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to report it.

SAR reports: By law, Alpine and its employees cannot disclose to the customer or anyone other than authorized parties that it has filed a SAR or provide information that would reveal the existence of a SAR. Questions regarding SAR filings should be referred to Compliance. If you become aware of an unauthorized disclosure of an SAR or you receive a subpoena for an SAR, **immediately contact the Compliance Department**. Designated Compliance personnel will be responsible for contacting FINCEN to report the unauthorized disclosure.

9.7.7.1 Role Of Operations Personnel

Operations personnel are an important first line of defense in preventing transactions with sanctioned parties. The following guidance is provided to assist Operations personnel in identifying blocked parties. Any questioned accounts or transactions should be referred to the AML Compliance Officer.

- On a monthly basis, the AML Compliance Officer shall provide a current list of countries included on the OFAC list. These are countries considered potential havens for money laundering, drug trafficking, or terrorist activities. Information is included on the OFAC web site at *www.treas.gov/ofac*.
- On a periodic basis, the AML Compliance Officer shall provide a current list of countries included on the Financial Action Task Force (FATF) list. The Financial Action Task Force (FATF) is the global standard setting body for anti-money laundering and combating the financing of terrorism. In order to protect the international financial system from money laundering and financing of terrorism risks and to encourage greater compliance with their standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.
- When processing the opening of accounts, back office employees shall determine if new accounts have addresses as residents of countries included on the OFAC list and report any that appear on the list to the AML Compliance Officer.
- Questions regarding requests to transfer funds or securities to residents or entities domiciled in any country included on the OFAC list shall be reported to the AML Compliance Officer.

9.7.7.2 Role of Retail Brokerage Personnel

Retail sales personnel are also an important first line of defense in identifying, detecting and/or preventing transactions. Retail sales personnel is in a unique position of knowing the client best. It is important that you understand the customer's financial resources, business activities, and sources of funds to identify when purported or actual activity deviates from the standard transactions one expects to see in a customer account. The process of knowing the customer does not end at the time the account established. The process of knowing the customer continues through the ongoing maintenance of the client's account. Any questioned accounts or transactions should be referred to the AML Compliance Officer or designee.

9.8 Currency Reporting Requirements

[SEC Securities Exchange Act of 1934 Rule 17a-8; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart C; FinCEN pamphlet on CTR reporting: http://www.fincen.gov/whatsnew/html/20090224.html]

The Bank Secrecy Act requires broker-dealers to report certain transactions relating to currency transactions, as follows:

- Report cash or currency deposits of more than $10,000, including multiple deposits on the same day that would total more than $10,000. A currency Transaction Report (CTR) is filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department. Some state regulators also require reporting of currency transactions.
- Report currency or bearer instruments over $10,000 transferred into or out of the U.S. The Currency and Monetary Instrument Transportation Report (CMIR) is filed with the U.S. Customs Service.

The following summarizes the reporting requirements under the Bank Secrecy Act. Alpine's CFO is responsible for maintaining records of any currency reports required to be filed by Alpine and retaining them for five years.

9.8.1 Transactions Involving Currency Over $10,000

If Alpine accepts a currency deposit exceeding $10,000, it is required to file a Currency Transaction Report (CTR) with the Financial Crimes Enforcement Network (FinCEN). Multiple transactions by the same person equaling over $10,000 in any one day must also be reported. Alpine's Operations Principal is responsible for filing these reports and maintaining records of them for a period of five years from the filing date.

The back office is responsible for receiving currency and will process these requests in accordance with their standard operating procedures. Currency deposits in the amount greater than $10,000 will be reported to the AML Officer. Multiple transactions by the same person equaling over $10,000 in any one day must also be reported to the AML Officer. The AML Officer will notify Alpine's Operations Principal to complete the required filings.

"Currency" is defined as the coin and paper money of the U.S. or legal tender of other countries. Currency also includes U.S. silver certificates, U.S. notes, federal reserve notes, and official foreign bank notes customarily used and accepted as a medium of exchange in a foreign country.

9.8.2 Transactions Involving Currency Or Bearer Instruments Over $10,000 Transferred Into Or Outside The U.S.

Broker-dealers are required to file a Currency and Monetary Instrument Transportation Report (CMIR) with the U.S. Customs Service to report transactions in physical currency and/or bearer instruments which alone or in combination exceed $10,000 and which are shipped or transported into or outside

the U.S. This filing is not required for currency or other monetary instruments mailed or shipped through the postal service or by common carrier. Alpine's Operations Principal is responsible for filing these reports and maintaining records of them for a period of five yeras from the filing date.

9.8.3 Prohibition Against Structuring Deposits To Avoid Reporting

Cash or currency deposits or attempted deposits which appear to be part of a deposit structure to avoid IRS or Customs currency reporting requirements or Alpine's limitations, or are otherwise suspicious, may not be accepted and must be reported to the Branch Manager. Employees are prohibited from:

- aiding or advising a customer in structuring a transaction to avoid reporting requirements
- holding instruments for deposit on succeeding days
- transporting cash or cash equivalents or bearer instruments to a bank on behalf of a customer

9.8.4 State Reporting Requirements

States have adopted various currency and suspicious activity reporting requirements. Most states have entered into an agreement with FinCEN to provide them with duplicate copies of forms filed by broker-dealers. Some states, however, require duplicate filing with the states themselves at the time the broker-dealer files with a federal agency. Alpine's CFO will file reports as required under state requirements.

9.9 Foreign Financial Account Reporting Requirements And Recordkeeping (FBAR)

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart C; Form: http://www.fincen.gov/forms/files/f9022-1_fbar.pdf; FinCEN Notice 2012-1]

Certain "United States persons" that maintain accounts (including any account where the person has a financial interest in, or signature or other authority over) in foreign jurisdictions and with aggregate balances exceeding $10,000 are required to file a Report of Foreign Bank and Financial Accounts (FBAR) Department of Treasury Form 90-22.1 with FinCEN on or before June 30th of each calendar year for accounts maintained during the previous calendar year. Certain U.S. persons with signature authority over, but no financial interest in, foreign financial accounts of their employers and entities related to their employers have an extension until June 30, 2013 to file Form 90-22.1 (see FinCEN Notice 2012-1). The FINOP is responsible for filing the annual report if it is required for Alpine.

The filing requirement applies to:

- Non-resident aliens and foreign entities "in and doing business" in the U.S.
- All forms of U.S. business entities, trusts, estates with foreign accounts.
- U.S. citizens and residents with signature or other authority over a foreign account.
- Trust beneficiaries with a greater than 50% beneficial interest in a trust with a foreign account.
- U.S. citizens and resident stockholders with greater than 50% of the value or vote of the shares of a corporation with foreign accounts.
- Entities that are disregarded for tax purposes, such as limited liability companies.

The filing requirement does not apply to certain entities or situations. The regulation should be consulted for specific exemptions or conditions of exemptions.

- If the account is maintained in the United States, it is not considered a foreign account even if it holds foreign assets.

- An omnibus account held by a custody bank that holds assets both in the U.S. and outside the U.S. is not considered a foreign account unless the customer has direct access to its foreign holdings maintained at the foreign institution.
- Certain entities are excluded including: foreign hedge funds, venture capital funds, or private equity funds; tax-exempt investors that own offshore "blocker corporations;" government pension funds; pension plan participants and IRA owners (provided the trustee files a FBAR); investment advisers and employees of such advisers that provide advice to SEC-registered entities; remainder interests in trusts and beneficiaries of discretionary trusts; employees of a U.S. or foreign entity that issued a class of foreign equity (including ADRs) registered with the SEC.

There also are exemptions for officers or employees with signature or other authority over certain foreign financial accounts but no financial interest in the reportable account. The regulation should be consulted for details regarding who is not required to notify FinCEN regarding signature or other authority over such an account.

9.10 Recordkeeping Requirements

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D]

In addition to maintaining records of reports filed with the IRS or other authorities, broker-dealers are obligated to maintain records of certain transactions, for potential inspection by regulators and other authorities. These records must be retained for five years.

9.10.1 Fund Transfers And Transmittals

[Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart D; FINRA Notice to Members 97-13, 96-67 and 95-69; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advissu7.pdf; SEC Q&As: http://www.sec.gov/about/offices/ocie/aml2007/fincen-advsiii.pdf]

Broker-dealers are required to collect and retain information (such as name, address, account number of customer, date and amount of wire, payment instructions, name of recipient institution, and name and account information of wire payment recipient) and maintain records for domestic and international funds transfers (including wire fund transfers) of $3,000 or more, with certain exceptions. This includes transfers between accounts that are not for the same owner and transfers to third parties including banks and other financial institutions. Records of transfers are available for inspection by regulators and other appropriate authorities, when requested.

Alpine (and its clearing firm or other third party, if applicable) is responsible for complying with the requirements to record information regarding fund transfers and, when required, verifying information regarding transmitters and recipients who are not established customers. Examples of verification information include:

- Name and address
- ID reviewed (type and number on the ID)
- Taxpayer ID number (or alien ID or passport number including country of issuance)
- Copy or record of method of payment (*e.g.,* credit card, check)

9.10.2 Other Recordkeeping Requirements

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart D 1023.410]

The Bank Secrecy Act incorporates other records requirements that include records covered by *Books And Records* in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*. Alpine will retain all of the following required records:

1. Trading authorizations which are addressed in the chapter *ACCOUNTS*
2. Records under 17a-3 which are addressed in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*
3. A record of each receipt of currency, other monetary instruments, checks, or investment securities and of each transfer of funds or credit, of more than $10,000 received on any one occasion directly and not through a domestic financial institution, for any person, account or place outside the United States.

9.11 Detecting Potential Money Laundering

Responsibility	• AML Compliance Officer • Other designated supervisor for review of AML Compliance Officer accounts
Resources	• Internal reports of transactions, available exception reports
Frequency	• Daily and ongoing
Action	• Review reports of transactions (cash and security transactions) to identify potential money laundering (including employee accounts) • Another designated supervisor will review the AML Compliance Officer's accounts • Report suspicious activity (see the policy in this chapter) • Notify RRs, supervisors, and close accounts when necessary
Record	• Reports reviewed • Action taken, when necessary • Suspicious activity reports

Alpine has an ongoing program to identify potential money laundering. Monitoring will be conducted using available exception reports or review of a sufficient amount of account activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or involve "red flags" (indicators of potential money laundering) which are included in the *Money Laundering* policy in the chapter *GENERAL EMPLOYEE POLICIES*. Items reviewed include trading and wire transfer transactions in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer. Among the information used to determine whether to file a suspicious activity report are exception or transaction reports that include transaction size, location, type, number, and nature of the activity.

Trading accounts will be identified and monitored where a series of financial transactions may help obscure the origins of the funds. This may include effecting securities transactions, closing the account, and transferring funds to a bank or other account, particularly to an offshore location. Trading penny stocks (which may involve unregistered distributions) or engaging in retail forex trading will, in particular, be monitored when they occur.

Alpine has included an educational policy *(Money Laundering)* in the chapter *GENERAL EMPLOYEE POLICIES* to educate employees on money laundering and guidelines for detecting money laundering activities. Periodically detection of money laundering and the obligation to report suspicious activities will be included in continuing education and other educational programs for employees.

9.11.1 Foreign Currency Transactions

Foreign financial institutions may purchase U.S.-denominated bonds, generally issued by foreign governments, with the local currency, which are then transferred to a U.S. broker-dealer and sold, with proceeds then transferred offshore. U.S. broker-dealers act as intermediaries in these transactions and may receive foreign bonds or other securities worth millions of U. S. dollars without knowing who or how many underlying customers may be involved. RRs and [The Firm] must be diligent about such transactions which may involve money laundering.

9.12 Information Sharing Between Financial Institutions

[USA PATRIOT Act Section 314(b); Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; FinCEN certification: http://www.fincen.gov/fi_infoappb.html]

Alpine does not share information with other financial institutions regarding accounts and account activity unless it has filed the requisite certification with the Financial Crimes Enforcement Network ("FinCEN") to allow Alpine to share information pursuant to Section 314(b) of the USA PATRIOT Act. Alpine may share information with an affiliated company, including its parent company, if the financial institution has filed a current 314(b) form with FinCEN.

9.13 Alpine's Employee Reporting Obligations

All employees are obligated to promptly report to the AML Compliance Officer or designee any known or suspected violations of anti-money laundering policies as well as other suspected violations or crimes. If the potential violation implicates the AML Officer, it should be reported to a senior officer of Alpine. All reports are confidential and the employee will suffer no retaliation for making them.

What to report: Crimes or suspected crimes by individuals (whether associated with Alpine, a customer, or prospective customer) are required to be reported. This includes suspicion that Alpine is being used as a conduit for criminal activity such as money laundering or structuring transactions (discussed below) to evade the Bank Secrecy Act reporting requirements. There is no clear definition of what constitutes a "crime." If you believe some improper or illegal activity is occurring, it is your obligation to be attentive and alert to the red flags and report to the AML Compliance Officer or designee any new or existing customers who may be engaged in violations of anti-money laundering regulations.

SAR reports: By law, Alpine and its employees cannot disclose to the customer or anyone other than authorized parties that it has filed a SAR or provide information that would reveal the existence of a SAR. Questions regarding SAR filings should be referred to Compliance. If you become aware of an unauthorized disclosure of an SAR or you receive a subpoena for an SAR, **immediately contact the Compliance Department**. Designated Compliance personnel will be responsible for contacting FINCEN to report the unauthorized disclosure.

9.14 Suspicious Activity Reports (SARs)

[USA PATRIOT Act Sec. 356; FinCEN Guidance on Suspicious Activity Report Supporting Documentation: http://www.fincen.gov/Supporting_Documentation_Guidance.pdf; FinCEN Guidance FIN-2008-G005]

Responsibility	• AML Compliance Officer
Resources	• Reports from employees of crimes or suspected crimes • Suspicious activities detected through ongoing reviews • Other available information
Frequency	• As required
Action	• Review and investigate suspicious transactions referred by employees • Determine whether Alpine will file a SAR • If appropriate, file Form SAR-SF with FinCEN and state authorities • Notify senior management, as appropriate, of forms filed
Record	• Notes and other documented reviews are retained in a suspicious activity file • Copies of SARs filed by Alpine are retained in the SAR file with notation of when and to whom sent

Alpine will file Suspicious Activity Reports (SARs) for transactions that may be indicative of money laundering activity. Suspicious activities include a wide range of questionable activities. Examples may include, but are not limited to, trading that constitutes a substantial portion of all trading for the day in a particular security; trading or journaling between/among accounts, particularly between related owners; late day trading; heavy trading in low-priced securities; unexplained wire transfers, including those to known tax havens; unusually large deposits of funds or securities; shares of physical securities of low-priced securities that have an issue date of less than 12 months and are more than one million shares or have a market value over a certain amount.

Determining whether an activity or series of activities is suspicious is a facts and circumstance analysis. Such determinations will be made by the AML Compliance Officer or designee.

9.14.1 Potential Risk Indicators

[NASD Notice to Members 02-21]

The following are examples of risk indicators (red flags) that may suggest potential money laundering.

Red Flags indicating potential Money Laundering
The customer exhibits unusual concern regarding Alpine's compliance with government reporting requirements and Alpine's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business strategy.
The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
The customer (or a person publicly associated with the customer) has a questionable background

or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
The customer engages in suspicious activity involving the practice of depositing penny stocks, liquidates them, and wires proceeds. A request to liquidate shares may also represent engaging in an unregistered distribution of penny stocks which may also be a red flag. [FINRA Regulatory Notice 09-05]
The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from Alpine's policies relating to the deposit of cash and cash equivalents.
The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).
The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
The customer's account shows numerous currency or cashiers check transactions aggregating to significant sums.
The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven
The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
The customer requests that a transaction be processed in such a manner to avoid Alpine's normal documentation requirements.
The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent business purpose or other purpose.
The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

9.14.2 Identifying Potential Suspicious Activity

Alpine uses a number of tools to identify potential suspicious activity including:

- Transaction information including disbursement of funds or securities are reviewed periodically by the Branch Manager and AML compliance officer.
- The AML Compliance Officer provides education to Alpine's RR, to Supervisors approving new accounts, operations personnel and to the Branch Manager.
- Employee reports of potential suspicious activity are given to the AML Compliance Officer
- It is always at the manager or AML Compliance Officer's discretion, when taking into consideration all factors, when a SAR Form should be filed.

All employees have an ongoing obligation to report potentially suspicious activity to the AML Officer or designee.

9.14.3 When A Report Must Be Filed

A SAR must be filed for any transaction that, alone or in aggregate, involves at least $5,000 in funds or other assets, if Alpine knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is part) falls into one of the following categories:

- Transactions involving funds derived from illegal activity or intended or conducted to hide or disguise funds or assets derived from illegal activity.
- Transactions designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act (BSA).
- Transactions that appear to serve no business or apparent lawful purpose or are not the sort of transactions in which a particular customer would be expected to engage, and for which Alpine knows of no reasonable explanation after examining the available facts.
- Transactions that involve the use of Alpine to facilitate criminal activity.

Excluded from the filing requirement are violations otherwise reported to law enforcement authorities such as:

- a robbery or burglary that is reported to law enforcement authorities
- lost, missing, counterfeit, or stolen securities reported pursuant to 17f-1
- a violation of federal securities laws or SRO rules by Alpine, its officers, directors, employees, or RRs that are reported to the SEC or SRO, except for violations of Rule17a-8 (filing of Currency and Transaction Reports) which must be reported on a SAR

9.14.4 Filing A Report And Emergency Notification

If Alpine determines to file a SAR with FinCEN, the AML Compliance Officer will file:

- within 30 days of becoming aware of the suspicious transaction; or
- if no suspect has been identified within 30 calendar days of detection, reporting may be delayed an additional 30 calendar days or until a suspect has been identified, but no later than 60 days from date of initial detection.

In situations involving violations that require immediate attention (such as terrorist financing or ongoing money laundering schemes), the AML Compliance Officer will immediately notify by telephone an appropriate law enforcement agency. Suspicious transactions that may relate to terrorist activity may also be reported to FinCEN's Financial Institutions Hotline. In either event, a SAR will be filed.

9.14.4.1 Emergency Notification

[FINRA Notice to Members 02-21]

When conducting due diligence or opening an account, Federal authorities will be notified immediately by the AML Compliance Officer, when necessary, in the following situations:

- A legal or beneficial account holder or person is engaged in a transaction listed on or located in a country or region listed on the OFAC list.
- An account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list.
- A customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity.
- There is reason to believe a customer is trying to move illicit cash out of the government's reach.
- There is reason to believe the customer is about to use funds to further an act of terrorism.

Emergency contacts include:

- OFAC Hotline
- Financial Institutions Hotline
- Local U.S. Attorney's office
- Local FBI office
- Local SEC office

9.14.5 Retention Of Records

The AML Compliance Officer maintains a file of copies of SARs filed with FinCEN and all related documents for a period of 5 years from the filing date.

9.14.6 Providing SARs Information To SROs

[SEC letter to CEOs: http://www.sec.gov/about/offices/ocie/brokerdealerletter.htm]

While SARs are to be treated as confidential, [The Firm] will provide SARs and supporting documentation available to any self-regulatory organization (SRO) that examines [The Firm] for compliance with the SAR Rule, upon request of the SEC. The request may be part of a routine examination, an investigation, or part of the SRO's risk assessment effort within its examination program.

9.14.7 Prohibition Against Disclosure

By statute and regulation, Alpine may not inform customers or third parties that a transaction has been reported as suspicious. U.S. Treasury and Federal Reserve Board regulations also require Alpine to decline to produce SARs in response to subpoenas and to report to FinCEN and the Federal Reserve Board the receipt of such requests and Alpine's response. Failure to maintain the confidentiality of SARs may subject an employee to civil and criminal penalties under Federal law. Violations may be enforced through civil penalties of up to $100,000 for each violation and criminal penalties of up to $250,000 and/or imprisonment not to exceed five years. Alpine may also be liable for civil money

penalties resulting from AML deficiencies that led to improper SAR disclosure up to $25,000 per day for each day the violation continues.

Procedures to protect the confidentiality of SARs include the following:

- Access to SARs is limited to employees on a "need-to-know" basis
- SARs will be maintained in locked physical or electronic files
- SARs may not be left on desks or on open computer files and must be viewed without access by unauthorized persons
- SARs shared with others will be clearly marked "Confidential"

Compliance (or Alpine's counsel) is responsible for responding to subpoena requests and Compliance will notify FinCEN and our primary federal regulator, where required by law.

9.14.7.1 Recipient Of An Unauthorized SAR Disclosure

If you become aware of an unauthorized disclosure of a SAR or if you receive a subpoena request for a SAR, immediately contact the Compliance Department. Compliance will contact FINCEN's Office of Chief Counsel at (703) 905-3590. We may also be required to contact our primary federal regulator.

9.15 Requests And Written Notices From Enforcement Agencies

Under the Bank Secrecy Act, financial institutions are required to respond to federal banking agency requests for information relating to anti-money laundering compliance. The Rule requires provision of information and account documentation for any account opened, maintained, administered or managed in the U.S. The AML Compliance Officer or designee maintains records of information provided in response to regulators' requests including the request, date of response, and information provided.

9.15.1 Federal Banking Agency Requests -- 120-Hour Rule

[USA PATRIOT Act Section 319(b)]

Upon receiving a request from a Federal banking agency, the AML Compliance Officer will provide the requested information within 5 days (120 hours) of receiving the request or will make available the information for inspection by the banking agency.

9.15.2 FinCEN Requests For Information

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart E; USA PATRIOT Act Section 314; FinCEN 314(a) Fact Sheet: http://www.fincen.gov/statutes_regs/patriot/pdf/314afactsheet.pdf]

Responsibility	• AML Compliance Officer
Resources	• Deposit records, purchase/sale records, account records, other records as required
Frequency	• Upon request
Action	• Conduct a search of the required records • If a match is found, submit the Subject Information Form to FinCEN • Retain copy of 314(a) list received
Record	• Retain copies of the request

	• Notate records searched, and date of review and initial or sign the 314(a) list received • Information submitted (if a match is found) are retained in a FinCEN information request file • Sign or initial 314(a) Search Self-Verification Page and retain

The Financial Crimes Enforcement Network (FinCEN) sends law enforcement requests to financial institutions under Section 314(a) of the USA PATRIOT Act.

Requests for information from FinCEN will be forwarded to the AML Compliance Officer for response. Within 2 weeks of receipt of the request, if a match is identified with a named subject, the Subject Information Form (included with FinCEN's request) will be forwarded to FinCEN by electronic mail to *sys314a@fincen.treas.gov* or, if e-mail is not available, by fax at 703-905-3660.

FinCEN requests are confidential and may not be disclosed to the subject of the request. Alpine will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314; (2) to allow the AML Compliance Officer to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist Alpine in complying with any requirement of Section 314.

9.15.3 Foreign Bank Correspondent Accounts

[USA PATRIOT Act Section 313]

Upon receipt of a written request from a Federal law enforcement officer for information about a foreign bank correspondent account, the AML Compliance Officer will provide the requested information no later than 7 days after receipt of the request.

The AML Compliance Officer is responsible to terminate any correspondent relationship with a foreign bank within 10 business days of receiving a notice from the Treasury Dept. or the U.S. Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in a U.S. court.

9.16 Knowing the Customer

Being familiar with the customer's financial resources, business activities, and sources of funds are avenues for knowing the customer. The process of knowing the customer occurs at the time an account is opened as well as during the operation of a customer's account.

The identity of customers must be verified when a new account is opened. Procedures for verifying customer ID are explained in the chapter *ACCOUNTS* in the section *New Accounts*.

9.17 Customer Identification Program (CIP)

[USA PATRIOT Act Section 326; Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart B; FINRA Notice to Members 03-34; FinCEN Frequently Asked Questions: http://www.fincen.gov/cip_faq.html; FinCEN No-Action position on CIP requirements under clearing arrangements: FIN-2008-G002; Guidance on Obtaining and Retaining Beneficial Ownership Information, FinCEN Guidance, FIN-2010-G001 March 5, 2010]

The opening of new accounts is subject to customer identity verification requirements under Alpine's Customer Identification Program (CIP). Requirements for employees opening accounts as explained in the chapter *ACCOUNTS* are duplicated in this section to consolidate all AML requirements within this chapter.

The use of the term "customer" in this section is understood to include prospective customers.

9.17.1 Accounts Requiring Approval By The AML Compliance Officer

The following accounts require review and approval by the AML Compliance Officer at the time of opening. The AML Compliance Officer may require additional customer identification information for these accounts.

- **Numbered accounts** (accounts designating a number rather than a name as the account name).
- **Any account requesting confidential handling** of its name, mailing of confirmation and statements, *etc.*
- **Accounts domiciled in high risk countries.** Accounts domiciled in countries identified by OFAC or the Financial Action Task Force on Money Laundering (FATF) as having inadequate anti-money laundering standards or representing high risk for crime and corruption.
- **Foreign public officials.** Includes individuals in high offices of foreign governments, political party officials and their families and close associates (if known and/or readily identifiable).
- **Correspondent and Private Banking accounts.** See the section *Due Diligence For Correspondent And Private Banking Accounts.*

9.17.2 Customer Identity Verification

This section is duplicated from the Chapter 11.1.1

Responsibility	• Registered Principal
Resources	• New account application and other customer ID information
Frequency	• When accounts are opened
Action	• Before the Designated Supervisor approves an account, determine that customer identification (ID) verification information is included with the new account application and that it meets Alpine's requirements • For non-documentary verification, check the information included with the new account application for completeness and consistency with other customer-provided information (name, address, phone number, taxpayer ID number, *etc.*) • For unacceptable verification information (incomplete, inconsistent), return the application to the RR for further information or disapprove the account
Record	• Each Customer file shall contain the New Account Application and records that include customer ID verification as well as the Designated Supervisor's signature signifying approval

When opening new accounts, the customer's identity must be verified, as required by federal law. Customer identification (ID) information must be completed on the new account application.

Customer ID verification does NOT apply to accounts for:

- persons with an existing account at Alpine (unless the account requires approval by the AML Compliance Officer)
- banks
- governmental entities
- issuers of listed equity securities
- other financial institutions subject to regulation by the SEC, CFTC, Federal Reserve Board, OCC, FDIC, Office of Thrift Supervision, or the National Credit Union Administration
- persons opening accounts to participate in an ERISA plan

9.17.2.1 Required Customer Information

Basic information required by law **prior to opening the account** includes:

- **Name**
- **Date of birth,** for an individual
- **Address:**
  - for an individual, residential or business street address. If no street address exists or is available, an APO or FPO box number or the residential or business street address of a next of kin or another contact individual
  - for a non-individual (corporation, trust, *etc.*) a principal place of business, local office, or other physical location.
- **Taxpayer identification number** for a U.S. person (U.S. citizen or non-individual established or organized under U.S. or state laws).
- **Identification number for non-U.S. person** which may include a taxpayer ID number; passport number and country of issuance; alien identification card number; or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photo or similar safeguard.

In the case of a customer who has applied for a taxpayer identification number but has not yet received it, notation must be made on the new account application that the taxpayer ID has been applied for. The account will be restricted to liquidating transactions if the taxpayer ID number is not received within 30 days of opening the account.

9.17.2.2 Accounts For Individuals

When opening an account for an individual, a photo copy of an unexpired government-issued identification including a photo and residence address (such as a driver's liccense or passport), is required and made a part of the customer's account file.

9.17.2.3 Third Party Accounts

Customer ID required for third party accounts includes the following:

On behalf of an incompetent person: Obtain customer ID of the person holding power of attorney.

With power of attorney or trading authorization held by a third party: Obtain customer ID of the owner of the account. Customer ID is not necessary for the individual with authority over the account unless that person is unfamiliar to the RR or the circumstances regarding the opening of the account raises questions (customer requires wiring funds to an offshore address; third party is a foreign citizen; *etc.*).

9.17.2.3.1 Registered Investor Adviser Accounts

[SEC Division of Market Regulation No-Action Letter to SIFMA dated January 11, 2011: http://www.sec.gov/divisions/marketreg/mr-noaction/2011/sifma011111.pdf]

For accounts established by registered investment advisers, Alpine may rely on the adviser to have obtained information to comply with federal Customer Identification Program (CIP) rules under the following circumstances:

- it is reasonable to rely on the adviser's assurances;
- the adviser is federally regulated (state-only registered IAs do not qualify); and
- the adviser signs an agreement that it will annually certify to Alpine that it has implemented an anti-money laundering program and will perform (or its agents will perform) specified requirements of Alpine's CIP.

9.17.2.3.2 Omnibus And Sub-Accounts

Omnibus and sub-accounts are sometimes established by or on behalf of financial intermediaries for the purpose of executing transactions that will clear or settle at another financial institution or for delivering assets to the custody account of the beneficial owner at another financial institution. Limited information about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts to hold positions to be transferred to another financial institution. Transactions are initiated by the financial intermediary and the beneficial owner has no direct control over the omnibus or sub-accounts.

Under these circumstances, Alpine is not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder. In the event the customer's identity cannot be adequately verified using documentary and non-documentary methods, identity information on the persons or entities controlling the account will be required.

[SEC Q and A Regarding the Broker-Dealer Customer Identification Program Rule, October 1, 2003]
Omnibus and sub-accounts are sometimes established by or on behalf of financial intermediaries for the purpose of executing transactions that will clear or settle at another financial institution or for delivering assets to the custody account of the beneficial owner at another financial institution. Limited information about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts to hold positions to be transferred to another financial institution. Transactions are initiated by the financial intermediary and the beneficial owner has no direct control over the omnibus or sub-accounts.
Under these circumstances, Alpine is not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the accountholder. In the event the customer's identity cannot be adequately verified using documentary and non-documentary methods, identity information on the persons or entities controlling the account will be required.

9.17.2.4 Accounts For Non-Individuals

Account documents usually obtained for non-individual accounts (trust instruments, corporate authorization, partnership agreements, government-issued business license, *etc.*) will usually satisfy customer ID requirements. In the case of corporations, a corporate authorization is required. These documents must be obtained within 30 days of account opening to satisfy the requirement.

9.17.2.5 Non-Documentary Methods Of Verifying Customer Identification

Non-documentary methods of verifying customer ID involve other procedures. Non-documentary methods must be used in the following circumstances:

- An individual is unable to present acceptable photo ID.

- The documents presented are unfamiliar.
- The account is opened without obtaining documents.
- Other circumstances, at the discretion of the RR's supervisor, New Accounts, and/or the AML Compliance Officer, where Alpine is unable to verify the customer's identity.

In these circumstances, a non-documentary method must be indicated by the RR on the new account application:

- Direct customer contact information
- Information from a consumer reporting agency or other database
- References from another financial institution
- Obtained a financial statement from a bank
- Copy of a utility bill

9.17.2.6 Additional Verification For Certain Customers

For the following types of customers, a minimum of TWO forms of customer ID are required in addition to review and approval by the AML Compliance Officer **prior to** opening the account:

- Numbered accounts
- Accounts domiciled in high-risk countries included on the Treasury Dept. OFAC list (check with Operations personnel for a list of those countries or go to *http://www.ustreas.gov/offices/eotffc/ofac/sanctions/index.html*)
- Accounts for foreign public officials (individuals in high office in other countries, their families and close associates, political party officials)

9.17.2.7 Lack Of Customer ID Verification

For **customers presenting unacceptable customer ID** at the time of account opening, the account will not be opened.

For **accounts where non-documentary verification results in substantive, unresolved discrepancies** (information that is inconsistent such as name, address, taxpayer ID number, *etc.*), either the account will not be opened or will be immediately closed.

Where inability to verify raises questions about the customer, filing a Suspicious Activity Report will be considered (see the section *Suspicious Activity Reports*).

Questions regarding accounts that do not comply with requirements to verify customer ID should be referred to the AML Compliance Officer.

9.17.2.8 Customer Notice

Customers are provided notice, prior to opening an account, that their identification will be verified. This notice may be on Alpine's web site, on new account applications, or in other disclosures provided at the time of account opening.

9.17.3 Customer Identification Program Records

Customer identification verification records are retained with new account application records in accordance with rule recordkeeping requirements and the terms of the other financial institution's Customer Identification Program (CIP) including:

- information recorded on the new account application

- documentary verification including information from or copies of government-issued IDs or passports
- non-documentary verification
- account approval or disapproval
- resolution of discrepancies
- referral of the account to the AML Compliance Officer
- closing of an account that fails to meet CIP requirements
- other records as may be required

9.17.4 Comparison With Government Lists

As required by law, Alpine compares customer information against government lists. The section *OFAC List And Blocked Property* in the Anti-Money Laundering Program describes comparison of accounts with lists published by the Treasury Dept.

9.18 Identity Theft Prevention Program (FTC FACT Act Red Flags Rule)

[Fair and Accurate Credit Transactions Act (FACT Act) Section 114 and 315; FINRA Regulatory Notice 08-69; FINRA Red Flags Rule web site: http://www.finra.org/Industry/Issues/CustomerInformationProtection/p118480; Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation: http://www.govcollect.org/files/Appendix%20A%20to%20Part%20681.pdf]

Responsibility	• AML Compliance Officer
Resources	• New account information • Order records • Transaction information about cash or security transfers • Information reported by employees • Information from third party providers, customers, victims of identity theft, law enforcement agencies or others about potential identity theft
Frequency	• When new accounts are opened • When account addresses are changed • Ongoing - review of order records and transaction information • As received - employee information • As required - when a third party is engaged, confirm third party providers (including clearing firms) have identity theft program procedures which may be included in an affirmation in the third party's contract with Alpine • Annually - review of controls and procedures • Obtain senior management approval for any material changes to the program and any material changes to the policy • As needed - update program and provide revisions to senior mangaement for review and approval of material changes. Non-material changes to the Policy will not require senior management approval. • If directed by the CEO, provide revised procedures to the Board or Board committee • Annually - report to CEO • Annually (or more frequently) - provide training for employees

Action	• Establish and maintain the Identity Theft Program
	  ○ Provide initial Program and subsequent material changes to the Board, a Board Committee or CEO (if no Board exists) for review and approval
	  ○ Review controls and procedures annually as part of the

	annual testing described in the chapter *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*
	• Conduct reviews of orders and transactions to identify red flags
	• When red flags are identified, take corrective action which may include:
	  o Consultation with the RR and/or supervisor
	  o Monitoring the account
	  o Contacting the customer
	  o Changing passwords, security codes, or other security devices that permit access to an account
	  o Reopening an account with another account number
	  o Not opening a new account
	  o Closing an existing account
	  o Filing a Suspicious Activity Report
	  o Notifying law enforcement
	  o Taking no action if warranted
	• Conduct other reviews which may include:
	  o Periodic use of internet search engines to identify web sites using Alpine's or an RR's name
	  o Review online advertising to identify web sites for unauthorized links to promote stock fraud or that appear to be illegitimate
	• If Alpine's or an RR's identity is being used in a scam, take action which may include notifying regulators and the FBI, lodging a complaint at www.ftc.gov, and if it involves email solicitation or spoofing, forwarding email to spam@uce.gov
	• If a customer's account has been compromised, take action (described in a section that follows)
	• Include Identity Theft Prevention Program in the annual report to CEO (see the chapter *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*), reporting:
	  o Effectiveness of the policies and procedures in addressing the risk of identity theft
	  o Third party provider arrangements
	  o Significant incidents involving identity theft and management's response
	  o Recommendations for material changes to the Program
	• Review third party providers (including clearing firms) for adequacy of identity theft programs
	  o Contractually require them to have policies and procedures to detect Red Flags included in firm policies and report them to Alpine and/or take appropriate steps of their own to prevent/mitigate identity theft
	• Send confirmation of address change to the customer's old address when a change of address is made (see the section *Change Of Addresses On Accounts* in the chapter *FINANCIAL AND OPERATIONS PROCEDURES*)
	• Training:
	  o Include identity theft in AML training
	  o Develop training, identify target employees, and administer training

Record	• Policies and procedures and revisions • Reviews of orders and transactions with record of action taken • Red flags identified and record of action taken • Annual testing of procedures (see *SUPERVISORY SYSTEM,*

	PROCEDURES AND CONTROLS) • Annual report to CEO (see *SUPERVISORY SYSTEM, PROCEDURES AND CONTROLS*) • Confirmation that third party providers (including clearing firms) have adequate ITPPs and include in the contracts with third parties • Records of training including subjects included, date, who administered and who attended

9.18.1 Firm Policy

Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written Identify Theft Prevention Program (ITPP), which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 16 C.F.R. § 681.1(d).

9.18.2 ITPP Approval and Administration

Alpine's AML Officer is the designated identity theft prevention officer and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of this ITPP.

Alpine's Executive Committee will review and approve this ITPP whenever there are material modifications to the policy.

Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a).

9.18.3 Relationship to Other Firm Programs

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, and our Customer Identification Program (CIP) and red flags detection under our Anti-Money Laundering (AML) Program in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

Rule: 16 C.F.R. § 681.1, Appendix A, Section I.

9.18.4 Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks

likely to occur, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II.

9.18.5 Detecting Red Flags

We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML policies and procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III.

9.18.6 Preventing and Mitigating Identity Theft

We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely to occur. Based on this and our review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

9.18.6.1 Procedures to Prevent and Mitigate Identity Theft

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Applicants. For Red Flags raised by someone applying for an account:

1. Review the application. We will review the applicant's information collected for our CIP under our AML Program (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Get government identification. If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport.
3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    a. Contacting the customer

b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker or the Social Security Number Death Master File.
c. Checking references with other affiliated financial institutions, or
d. Obtaining a financial statement.

4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
5. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to FINRA, ; the SEC and State regulatory authorities.
6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice under state law.

Access seekers. For Red Flags raised by someone seeking to access an existing customer's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.
4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
   a. Firm information (both introducing and clearing firms):

i. Firm name and CRD number

ii. Firm contact name and telephone number

   b. Dates and times of activity
   c. Securities involved (name and symbol)
   d. Details of trades or unexecuted orders
   e. Details of any wire transfer activity
   f. Customer accounts affected by the activity, including name and account number, and
   g. Whether the customer will be reimbursed and by whom.
6. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to FINRA; the SEC; and State regulatory authorities.
7. Notification. If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers and to others where required by law or regulation.
8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that our response to a data breach does not limit or eliminate our insurance coverage.

9. Assist the customer. We will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Offering to change the password, security codes or other ways to access the threatened account;
    b. Offering to close the account;
    c. Offering to reopen the account with a new account number;
    d. Not collecting on the account or selling it to a debt collector; and
    e. Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Rule: 16 C.F.R. § 681.1(d)(iii) and Appendix A, Section IV.

9.18.7 Alpine Employees Reporting Obligations

Identity thieves use someone's personal identifying information to open new accounts and misuse existing accounts. Alpine has established an Identity Theft Prevention Program (ITPP) to help detect and prevent identity theft. Many elements of detecting or preventing identity theft utilize similar techniques to that of the anti-money laundering (AML) requirements included within these policies.

The ITPP is based on identifying "red flags" which may indicate an occurrence of identity theft. ***It is the responsibility of all employees to be attentive and alert to the red flags and report to the AML Compliance Officer any new or existing customers who may be engaged in violations of anti-money laundering regulations, identity theft or who have reported an instance of identity theft.***

For a list of potential identity theft red flags, refer to the section titled "*Red Flag Identification and Detection Grid*" located in the ***Identity Theft Prevention Program (FTC Fact Act Red Flags Rule)*** section.

9.18.8 Service Providers

We may use other service providers in connection with our covered accounts. In the event we utilize other service providers, we have a process to confirm that any other service provider that performs activities in connection with our covered accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by contractually requiring them to have policies and procedures to detect Red Flags and report detected Red Flags to us or take appropriate steps of their own to prevent or mitigate the identify theft.

Rule: 16 C.F.R. § 681.1(e)(4) and Appendix A, Section VI.(c).

9.18.9 Internal Compliance Reporting

Firm staff responsible for developing, implementing and administering our ITPP will report at least annually to our Executive Committee on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP.

Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.(b).

9.18.10 Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, our firm will review this ITPP annually, to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm.

Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b).

9.18.11 Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Our staff who deal with customers and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with customers and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with customers and their supervisors will ensure that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with customers and their supervisors will ensure that the identification presented and other information we have on file from the account.
9. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with customers and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
Category: Suspicious Personal Identifying Information	

10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources	If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match.
11. Inconsistencies exist in the information that the customer gives us	Our staff will check personal identifying information presented to us to make sure that it is internally consistent
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff may validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and may call the phone numbers given to ensure they are valid and not for pagers or answering services.
14. The SSN presented was used by someone else opening an account or other customers.	Our staff may compare the SSNs presented to see if they were given by others opening accounts or other customers.
15. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff may compare address and telephone number information to see if they were used by other applicants and customers.
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.
17. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file.
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet (or consumer credit report, if applicable) or cannot answer a challenge question.	Our staff may authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.

Category: Suspicious Account Activity	
19. Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	We will verify change of address requests by sending a notice of the change to the old addresses so the customer will learn of any unauthorized changes and can notify us.
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of securities easily converted into cash, if margin is permitted.	We will review new account activity to ensure that payments are made, and that credit is primarily used for securities easily converted into cash, if margin is permitted.
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending patterns, or electronic funds transfers (if applicable).	We will review our accounts periodic basis and look for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or changes in spending patterns or electronic fund transfers (if applicable).
22. An account that is inactive for a long time is suddenly used again.	We will review our accounts on a periodic basis to see if long inactive accounts become very active.
23. Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account and immediately check the account's activity.
24. We learn that a customer is not getting his or her paper account statements.	We will record on the account any report that the customer is not receiving paper statements and immediately investigate them.
25. We are notified that there are unauthorized charges or transactions to the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report.

Category: Notice From Other Sources	
26. We are told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report.
We learn that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the customer to learn the details of the unauthorized access to determine if other steps are warranted.

9.19 Due Diligence For Correspondent And Private Banking Accounts

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 312 and 313; FinCEN Fact Sheet (http://www.fincen.gov/312factsheet.pdf); FinCEN guidance regarding Rule 312 due diligence requirements: http://www.sia.com/moneyLaundering/pdf/SIA-FIAfromFinCEN05-02-06.pdf]

Responsibility	• AML Compliance Officer
Resources	• New account application • Foreign bank certification • Information about a foreign bank subsequent to opening that indicates it is a foreign shell bank where an account may not be maintained
Frequency	• As required when accounts are opened • Monthly - review of accounts identified for due diligence reviews

Action	• Conduct due diligence for correspondent and private banking accounts
	• For foreign bank accounts:
	  ○ Review certification to determine:
	  ▪ All required information is included
	  ▪ Inconsistencies (*i.e.*, location of the foreign bank's regulated affiliate is consistent with the designated banking authority that supervises the foreign bank and its regulated affiliate)
	  ○ Ensure procedures are in place to restrict transactions in accounts that do not provide certification within 30 days of opening the account
	  ○ Close existing prohibited accounts for foreign shell banks
	  ○ Review re-certifications
	  ○ Ensure procedures are in place to re-certify foreign banks within three years of original certification

Record	• Record of the AML Officer's review is maintained in new account

	records on the applicable form: o New account application o Certification form o Re-certification form • Records of closing or restricting accounts are retained with new account records

Due diligence requirements apply when opening and handling correspondent and private banking accounts that are maintained in the U.S. for non-U.S. persons. "Enhanced due diligence" is required for:

- Correspondent accounts for foreign banks in jurisdictions of money laundering concern or operating under an off-shore license
- Private banking accounts for senior foreign political figures

The purpose of these requirements is to detect and report known or suspected money laundering activity.

9.19.1 Definitions

Correspondent account: Includes any account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign institution, or to handle other financial transactions related to such foreign financial institution. This type of account presumes a formal relationship through which the financial institution provides regular services.

Private banking account: A private banking account is an account that is established or maintained for the benefit of one or more non-U.S. persons, requires minimum aggregate deposit of funds or other assets of not less than $1,000,000, and is assigned to a bank employee who is a liaison between the financial institution and the non-U.S. person. If the account otherwise satisfies the definition but the institution does **not** require a minimum balance of $1,000,000, the account does not qualify as a private banking account.

Senior foreign political figure includes:

- a current or former senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government, whether or not they are or were elected officials
- a senior official of a major foreign political party
- a senior executive of a foreign government-owned commercial enterprise (Senior executives are individuals with substantial authority over policy, operations, or the use of government-owned resources.)
- immediate family members of the above, and those who are widely and publicly known (or actually known) close associates of a senior foreign political figure
- a corporation, business, or other entity formed by or for the benefit of one of the above individuals
- a person "widely and publicly known" as a close associate of such a person

Proceeds of foreign corruption: any asset acquired by, through, or on behalf of a senior foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and include any other property into which any such assets have been transformed or converted.

Foreign bank: defined under the Bank Secrecy Act as a bank organized under foreign law, or an agency, branch, or bank office located outside the United States. The term does not include an agent, agency, branch or office within the U.S. of a bank organized under foreign law.

Foreign shell bank: a foreign bank without a physical presence in any country.

Regulated affiliate: a foreign shell bank that (1) is an affiliate of a depository institution, credit union, or foreign bank that maintains a physical presence in the United States or a foreign country, as applicable; and (2) is subject to supervision by a banking authority in the foreign country regulating such affiliated depository institution, credit union, or foreign bank.

9.19.2 Due Diligence For Correspondent Accounts For Foreign Financial Institutions

Due diligence requirements apply to the following types of foreign financial institutions:

- Foreign bank
- Foreign branch of a U.S. Bank
- A business organized under a foreign law that, if located in the U.S., would be a securities broker-dealer, futures commission merchant, introducing broker in commodities, or a mutual fund
- A money transmitter or currency exchanger organized under foreign law

The Dept. of Treasury has established the following minimum due diligence requirements:

- determine whether the account is subject to enhanced due diligence
- assess the money laundering risk posed, based on risk factors
- apply risk-based policies, procedures and controls to each account, including periodic review of activity

Factors considered in determining due diligence include:

- nature of services provided to the account
- length of relationship
- the AML supervisory regime in the account's home country
- any information known or reasonably available about the account's AML record

Due diligence procedures include the following:

Correspondent accounts for foreign financial institutions are forwarded to the AML Compliance Officer, at the time of opening, for review.

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
    - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including source of revenue and assets, whether the person/entity has existing accounts with Alpine, length of time the RR has known the account, who referred the account, and other available information about account background and how the account came to Alpine.

- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.
    - File a SAR, if appropriate.
- If the account is approved for opening, determine whether ongoing review is necessary.
    - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer.
    - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

9.19.2.1 Enhanced Due Diligence For Foreign Banks

Enhanced due diligence is required for a correspondent account for a foreign bank that is operating:

- under an offshore license;
- in a jurisdiction found to be non-cooperative with international AML principles; or
- in a jurisdiction found to be of primary money laundering concern under the USA PATRIOT Act.

The following requirements apply:

Refer the account to the AML Compliance Officer to:

- conduct appropriate enhanced scrutiny;
- determine whether the foreign bank itself offers correspondent accounts to other foreign banks (*i.e.,* nested accounts) and, as appropriate, identify such foreign bank customers and conduct additional due diligence on them; and
- identify the owners of such foreign bank, if its shares are not publicly traded.
- determine whether the account appears on any OFAC list;
- approve or reject the account.
- determine whether ongoing review is necessary.
    - If yes, establish duplicate statements or other method for ongoing review.
- report the account, if appropriate.

9.19.2.2 Prohibition Against Correspondent Accounts For Foreign Shell Banks

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F; USA PATRIOT Act Section 313]

Alpine is prohibited from establishing, maintaining, administering, or managing a correspondent account in the United States for an unregulated foreign shell bank. The prohibition does not apply to a foreign shell bank that is a regulated affiliate. If an account is inadvertently opened for an unregulated foreign shell bank, the AML Compliance Officer must be notified and the account will be immediately closed.

9.19.2.3 Foreign Bank Certification

[FinCEN Frequently Asked Questions re Certification: http://www.fincen.gov/faqsguidance.pdf]

When opening an account for a foreign bank, Alpine is obligated to ensure the bank is not a foreign shell bank and must obtain information about the foreign bank's owners and an agent for service of process. The bank must complete the Foreign Bank Certification which must be submitted to the AML Compliance Officer with a copy of the new account application for review. Every three years the bank is also required to re-certify the information filed with Alpine.

9.19.2.4 Special Measures

[USA PATRIOT Act Section 311; Bank Secrecy Act 31 CFR Chapter X Part 1010 Subpart F; FINRA Notice to Members 06-41; FinCEN information on all special measures issued: http://www.fincen.gov/reg_section311.html]

Responsibility	• Designated Supervisor
Resources	• FinCEN notification of special measures against named entities • Transaction records • Customer account records
Frequency	• As required when notified by FinCEN
Action	• Establish blocks on opening accounts for named entities • Notify correspondent accountholders • Review transactions to identify indirect use of correspondent accounts and close such accounts
Record	• Notices from FinCEN • Notification to correspondent accountholders • Transactions reviewed, identification of indirect use, and action taken

Some foreign jurisdictions, foreign financial institutions, international transactions, or types of accounts are designated to be of "primary money laundering concern" by the Secretary of the Treasury. This designation obligates Alpine to take certain "special measures" against the primary money laundering concern. The Secretary of Treasury announces when an entity is considered to be a primary money laundering concern. These special measures include:

- A prohibition against opening or maintaining a correspondent account in the U.S. for or on behalf of the primary money laundering concern including at the time of announcement, review of existing account records to identify any prohibited accounts
- Notification to correspondent accountholders that the account may not be used to provide the primary money laundering concern with access to Alpine
- Reasonable steps to identify an indirect use of correspondent accounts by the primary money laundering concern by review of transaction-based records

9.19.3 Due Diligence For Private Banking Accounts

[Bank Secrecy Act 31 CFR Chapter X Part 1023 Subpart F]

Private banking accounts:

- include accounts established for a non-U.S. beneficial owner.
- include accounts where the beneficial owner is an individual:
  - who has a level of control over, or entitlement to, the funds in the account
  - who directly or indirectly controls, directs, or manages the account
  - for whom an account is established, maintained, or administered in the U.S.
- exclude accounts for hedge funds (and other pooled vehicles) and corporations (that are not personal investment companies ["PICs"]).
- include accounts for PICs and trusts for the benefit of individual owners.

Requirements for due diligence:

- Determine the identity of all nominal and beneficial owners of the private banking account.
- Determine the purpose and expected use of the account.
- Determine whether any such owner is a senior foreign political official.
- Determine the source(s) of funds deposited into the private banking account and the purpose and expected use of the account.
- Review the account activity:
  - to ensure consistency with information about the account.
  - to report suspected money laundering activity.

Factors considered in determining due diligence include:

- Is the client from a jurisdiction identified by the federal government as a jurisdiction subject to OFAC restrictions or as having weak AML controls?
- Is the customer's business cash intensive?

Alpine cannot rely on foreign institutions to perform due diligence for private banking accounts, and due diligence obligations are ongoing.

9.19.4 Enhanced Scrutiny For Accounts Of Senior Foreign Political Figures

Accounts for senior foreign political figures (including persons and entities defined in this section) are subject to enhanced scrutiny:

Prior to opening, the account is referred to the AML Officer for review and approval.

- Review the account's home country vs. OFAC lists of jurisdictions of money laundering concern and blocked persons.
  - If identified on an OFAC list, report the account and close it.
- Review new account information about the account including employment history, sources of income and assets, whether the person/entity has existing accounts with Alpine, length of time the RR has known the account, who referred the account, and other available information about account background of the account and how the account came to Alpine.
- If there is inadequate information or due diligence procedures cannot be performed, refuse to open the account or close an existing account.
  - File a SAR, if appropriate.
- If the account is approved for opening, determine whether ongoing review is necessary.
  - If ongoing review is appropriate, establish duplicate statements or another method for review of account activity by the AML Officer.
  - Review will include identifying patterns of securities transactions and securities/money transfers that may be indicative of money laundering activity, and report such activity if necessary and close the account.

9.20 Shell Companies

[FinCEN advisory on shell companies: http://www.fincen.gov/AdvisoryOnShells_FINAL.pdf]

Shell companies can represent a potential money laundering risk. Most shell companies are formed for legitimate business reasons, but some have been used for illicit purposes.

"Shell company" refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little or no independent economic value. Legitimate purposes including holding stock or intangible assets of

another business entity (such as subsidiary company shares) but are not engaged in active business operations or facilitating domestic and cross-border currency and asset transfers and corporate mergers. State laws allow shell companies to obscure company structure, ownership, and activities, so there is little transparency to enable Alpine to understand with whom they are dealing.

Agents that act as intermediaries or nominee incorporation services (NIS) can play a central role in creating, maintaining, and supporting shell companies. Some agents and NIS firms also provide individuals and businesses with nominee services that preserve the anonymity of underlying officers, directors, and stockholders.

Shell companies are subject to review which may include:

- Checking accounts and owners (if information is available) against OFAC restrictions (applies to all accounts)
- Obtaining information about underlying owners
- Obtaining assurances from the shell company representative that principals have been screened

9.20.1 Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the AML Compliance Officer, in which case the employee shall report to the firm's CCO. Alpine believes that compliance with the AML policies and procedures set forth herein are of paramount importance and must be facilitated by the firm. All employee reports concerning AML violations will be kept confidential and no employee ramifications will result from its strict adherence.